ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертацию Бородина Алексея Евгеньевича

«Межпроцедурный контекстно-чувствительный статический анализ для поиска ошибок в исходном коде программ на языках Си и Си++», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Целью диссертационной работы Бородина А.Е. является построение методов статического анализа для поиска ошибок в исходном коде программ. Методы должны масштабироваться до программ в миллионы строк исходного кода, при этом демонстрируя высокое качество истинных срабатываний (более 50%) и пропуск малого количества ошибок. Кроме того, методы должны быть применимы в промышленном цикле безопасной разработки программ, т.е. время выполнения анализа ограничено, как правило, рамками ночного тестирования (6-8 часов). Ищутся как ошибки времени выполнения программы, так и ошибки исходного кода, не проявляющиеся явно при выполнении, но влияющие на качество программы (например, избыточный код, мертвый код).

Актуальность выбранной темы обеспечивается тем, что в мире существует всего 2-3 коммерческих анализатора, отвечающих описанным критериям, их код закрыт, и используемые алгоритмы в деталях неизвестны. Анализатор Svace, разрабатываемый в Институте системного программирования РАН, также показывал нужное качество анализа для программ в сотни тысяч-единицы миллионов строк кода. Однако при переходе к программам в 5-10 млн. строк кода (ОС Android, Tizen) уровень истинных срабатываний резко упал, дальнейший анализ результатов также показал, что многие ошибочные ситуации были пропущены. Требовалось разработать новые алгоритмы, обеспечив необходимое качество анализа для этих программ.

К решению поставленной задачи Бородин А.Е. подошел системно. Во-первых, им были разработаны новые внутрипроцедурные алгоритмы ядра анализатора, вычисляющие наиболее важные данные о программе: значения и связи переменных (на основе варианта алгоритма нумерации значений) и множества потенциальных целей указателей. Выбранные алгоритмы обеспечивают как точность анализа, так и масштабируемость: добавление новых детекторов ошибок лишь незначительно увеличивает время анализа, т.к. большинство необходимой информации уже доступно, а для вычисления специфичных для детектора атрибутов программы, как правило, нужно обработать лишь некоторые инструкции программы. Кроме того, возникает и чувствительность к путям выполнения за счет сохранения условий, при которых возникают необходимые детекторам атрибуты.

Во-вторых, предложен алгоритм межпроцедурного анализа, который на основе данных внутрипроцедурных алгоритмов строит т.н. резюме процедуры – структуру данных, параметризованную входными параметрами процедуры, которая описывает влияние вызова процедуры на выполнение программы. При обработке вызовов уже проанализированных процедур нет необходимости возвращаться к анализу тела процедуры, достаточно использовать резюме процедуры с учетом конкретного контекста вызова. Таким образом, снова обеспечивается как точность анализа (за счет контекстной чувствительности при обработке вызовов и чувствительности к путям), так и масштабируемость (за счет алгоритмов создания резюме, сохраняющих лишь необходимую информацию, и за счет однократного анализа каждой процедуры).

Все предложенные диссертантом методы были реализованы в анализаторе Svace и показали необходимую точность и масштабируемость, давая полное решение поставленной задачи. Так, при сравнении разработанной версии анализатора с версией начала 2015 года количество выданных предупреждений для кода ОС Android версии 4 выросло в среднем в 6 раз, а уровень истинных срабатываний был сохранен (по важным видам ошибок он находится между 46% и 87%), часто – улучшен. В результате работы анализатор Svace был внедрен в цикл разработки крупной зарубежной компании.

При разработке и реализации методов, описанных в диссертации, Бородин А.Е. проделал большой объем работы, в том числе отсмотрел и проанализировал множество промышленного исходного кода, провел многочисленные эксперименты. Кроме того, Бородин А.Е. руководил группой исследователей, разрабатывающих детекторы конкретных ошибок на основе предложенных им методов анализа.

Считаю, что диссертационная работа соответствует всем требованиям, предъявляемым ВАК к работам на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, а ее автор, Бородин Алексей Евгеньевич, заслуживает присуждения ему ученой степени кандидата физико-математических наук.

Научный руководитель:
в.н.с. ИСП РАН, к.ф.-м.н. А. А. Белеванцев
28 марта 2016 года

Подпись Белеванцева А.А. удостоверяю

Директор ИСП РАН,
д.ф.-м.н.